Physical layer models and techniques for software radio

SPREAD SPECTRUM DIGITAL RADIO TRANSMISSION TECHNIQUES -

Prof. C. Regazzoni

DITEN - Department of Electrical, Electronic, Telecommunications Engineering and Naval Architecture

Bibliography

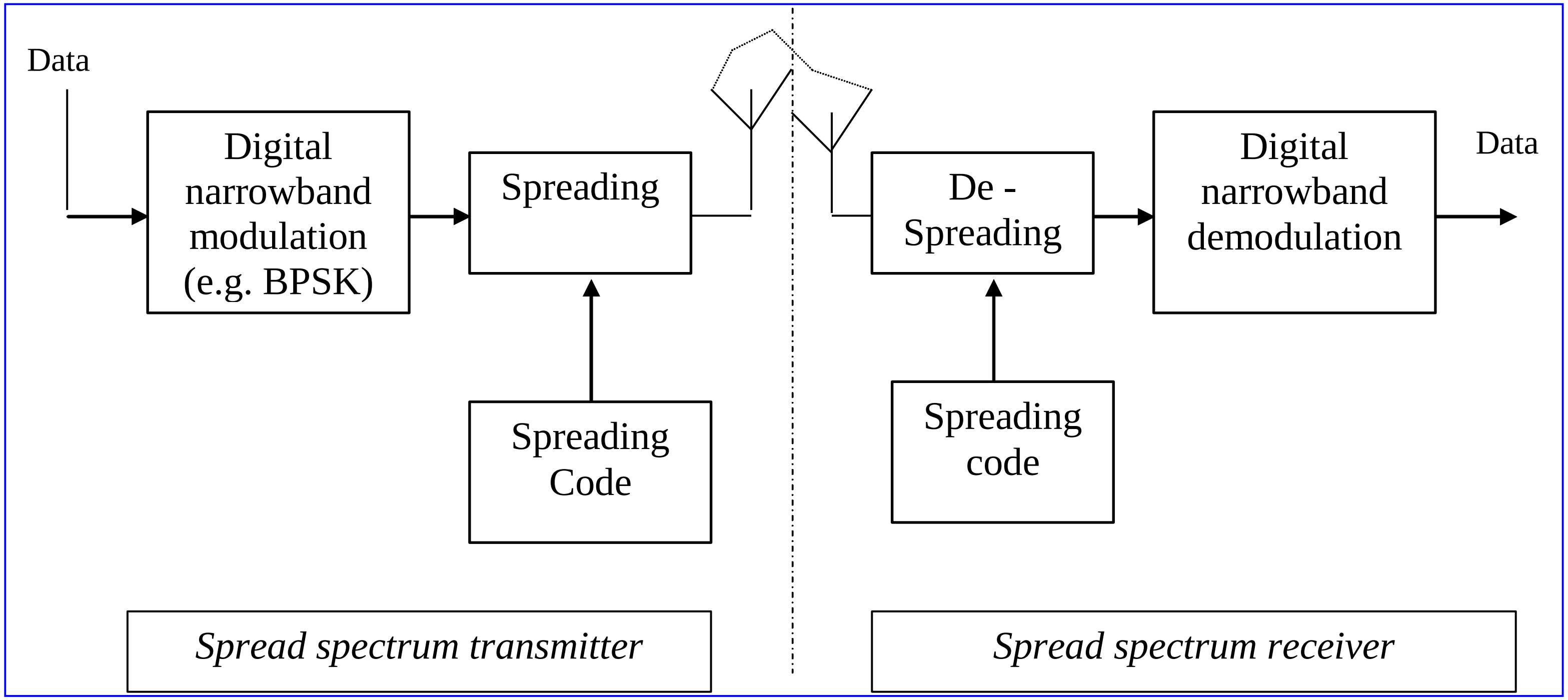
1. R. Pickholtz, D. L. Schilling, and L. B. Milstein, “Theory of Spread-Spectrum Communications – A Tutorial”, *IEEE Transactions on Communications,* Vol. COM-30, No. 5, Maggio 1982, pp. 855-884.
2. K. Pahlavan, A.H. Levesque, *“Wireless Information Networks”*, Wiley: New York 1995.
3. A.J. Viterbi, *“CDMA: Principles of Spread Spectrum Communications”*: Addison Wesley: 1995.
4. J.G. Proakis, *“Digital Communications”*, (Terza Edizione), McGraw-Hill: 1995.

Spread Spectrum

- Spread Spectrum is a Digital transmission technique.
- The signal is spread on a bandwidth W larger than the original one R.
- The spread signal is characterized by a very low power per frequency unit (Watt/Hertz).
- Process Gain P>1, is defined as the ratio between the bandwidth of Spread Spectrum signal (W) and the (narrower) bandwidth of the original signal (R)

$$P = \frac{W}{R}$$

SS System Architecture



Spread spectrum main properties and advantages (1/5)

1. High protection against illegal access
2. Low probability of random interception
3. High safety against intentional jamming
4. Multiple Access to the channel with multi user interference reduction
5. Multi path interference attenuation

Properties and Advantages (2/5)

<u>High protection against illegal access</u>

The signal is spread on a wide band by using a pseudo-random pattern,. i.e. the pseudo-noise PN sequence .

The PN sequence can be expressed as a sequence of elements called Chips (Chip Sequence)

It is known only to transmitter and receiver.

If this ‘key’ is not available, it is difficult to de-spread the narrow-band signal from the spread one and then to demodulate it.

Properties and Advantages (3/5)

<u>Low Probability of random Interception (LPI)</u>

Due to the very low power spectral density of the signal, the transmitted signal is almost not distinguishable from thermal noise, making it very difficult to be detected.

<u>High safety against jamming</u>

Effects of intentional narrowband interference against a transmitted signal (jamming) can be highly reduced by spreading a signal, and, in some cases, fully eliminated. To this end, Spread Spectrum techniques have been invented and extensively used during Second World War.

Properties and Advantages (4/5)

Multiple Access and multi-user interference reduction

By using different PN chip sequences for different users, it is possible for multiple users to share in time and frequency the same physical radio channel.

This technique is called Spread spectrum **CDMA** (*Code Division Multiple Access*), and is a powerful alternative to TDMA and FDMA.

By appropriately selecting PN codes of different users in SS-CDMA, Multi-User Interference (MUI) (i.e. interference among users) can be strongly reduced.

Some techniques can be used for this, like equalization of power at the receiver (Near-far power control) and selection of PN codes (e.g orthogonal spreading codes).

Properties and Advantages (5/5)

Multipath Self-Interference Reduction

The appropriate selection of PN codes can be also useful to minimize effects of time spread on wireless channels.

Self intereference by replicas of the same transmitted signal arriving at the receiver at different time and with different phases can be minimized by selecting PN random codes and related detection techniques.

Spread Spectrum techniques so can strongly reduce multipath effects, thus obtaining better results than narrowband modulations.

Applications

- Cellular Networks
- Wireless LAN
- Train-Ground communications
- Remote Video-Surveillance

Application	**Carrier**	**User Bandwidth**
Cellular Networks, WLAN	902–928 MHz	1.25 MHz (IS-95)
Wireless Multimedia, 3G (UMTS)	1.85-2.2 GHz	350MHz
Remote Video Surveillance, WLAN	2.4–2.4835 GHz	26 MHz (IEEE 802.11)
WLAN	5.725–5.850 GHz	Non standard

Main Spread Spectrum Techniques

Two methods are mainly used:

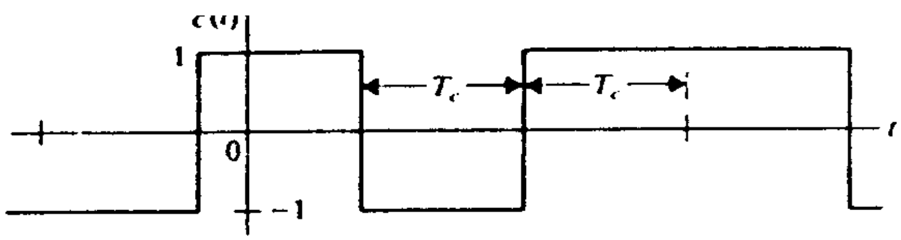
- **DIRECT SEQUENCE (DS)**
- **FREQUENCY HOPPING (FH)**

Hybrid methodologies have been also implemented

Direct Sequence (DS)

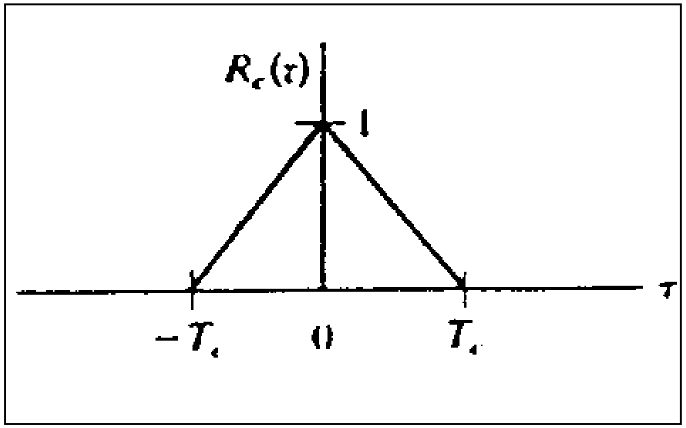
Direct Sequence Spread Spectrum (DS-SS) is based on direct base-band multiplication of

- digital signal at a data rate 1/T
- a higher-rate random base band sequence (pseudo noise PN sequence).
- The PN sequence varies at the maximum rate given by rectangular pulses of T_c (chip time) seconds.

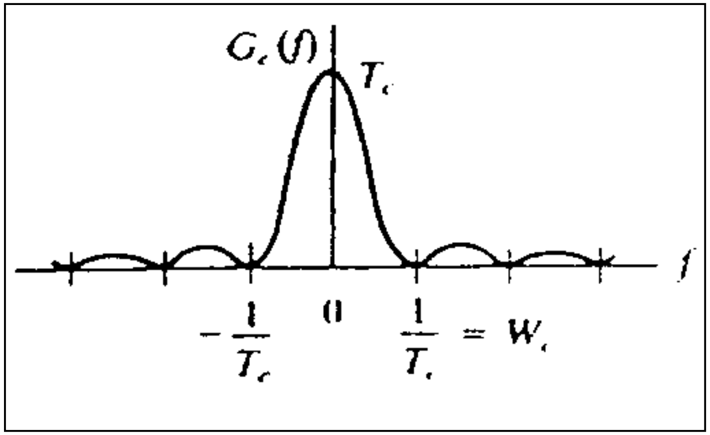


Direct Sequence (DS)

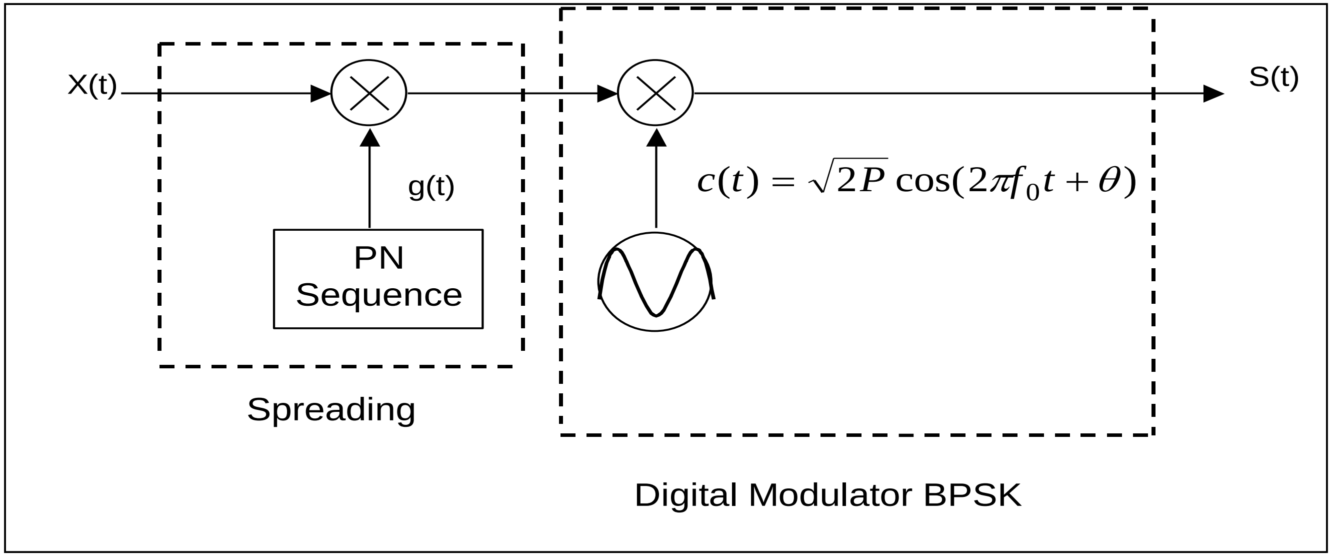
The auto-correlation function of the PN sequence has a memory equal T_c



The spectral density function (Fourier transform of the auto-correlation function) of the PN sequence has a bandwidth $1/T_c$ larger than 1/T



DS-SS Transmitter

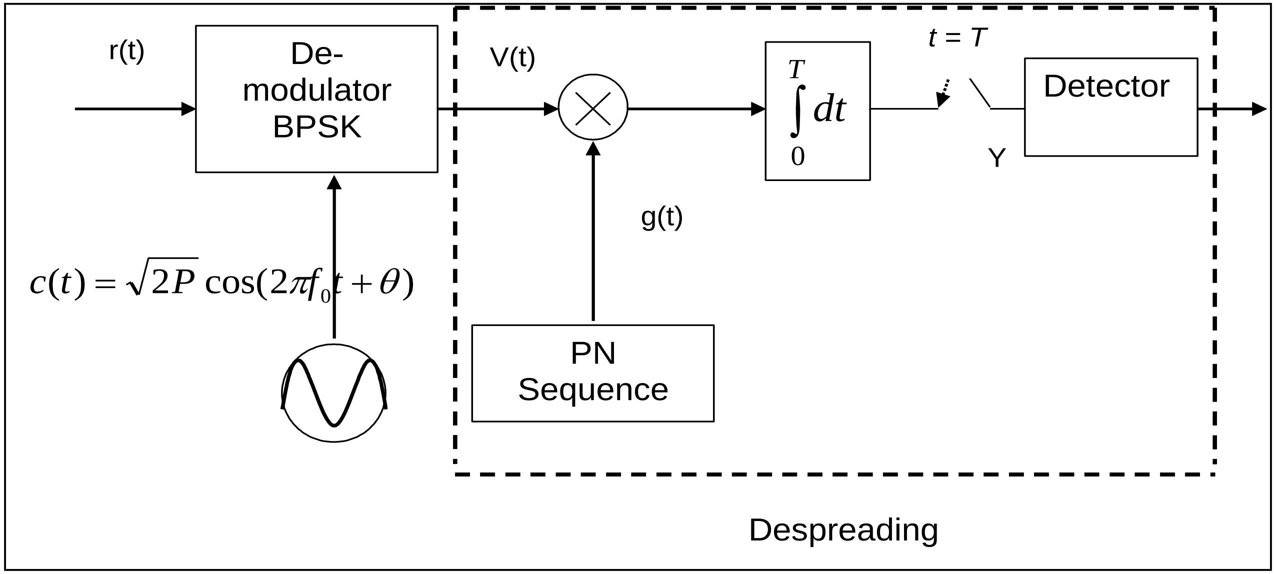


Let the source signal X(t) be a binary digital signal with period T. Spreading is performed by multiplying X(t) by PN sequence, g(t), choosing Tc as a integer multiple of T, i.e.

$$T_c = \frac{T}{N}$$

Spread signal is then modulated through a multiplication by a carrier c(t) with frequency f_0 and phase θ.

DS-SS Receiver



The receiver signal r(t) is composed by the transmitted S(t) corrupted by noise. With Additive White Gaussian Noise (AWGN), the received signal is

$$r(t) = S(t) + n(t) \qquad r(t) = \sqrt{2P}X(t)g(t)\cos(2\pi f_0 t + \theta) + n(t)$$

where n(t) is the Gaussian Noise with spectral density N_0.

DS-SS Receiver

The received signal r(t) is first BPSK demodulated.

The signal is multiplied by a carrier tone f_0 locally generated at the receiver and then filtered to remove the image frequency (at $2f_0$).

After demodulation the signal is:

$$V(t) = \sqrt{\frac{P}{2}} X(t) g(t) + n_{lp}(t)$$

where $n_{lp}(t)$ is the colored noise obtained by low-pass filtering n(t), with zero mean.

Demodulation allows one to obtain a baseband spread version of the signal X(t)

DS-SS Receiver

The despreading module follows, i.e. a **matched filter**, that compares a copy of the PN sequence with the incoming spread baseband noisy version of the data. The filter has to be synchronized.

Synchronization can be highly computationally demanding and requires good alignment performances, being very important in DS-SS, in order to perform a correct detection of each symbol of the signal.

The output of matched filter in *t*=*T* is a variable Y on which the decision module has to take its decision at each time KT, with K>0.

As $g^2(t) = 1$*,* in case the same PN code is used at the receiver as the one used at DS-SS transmitter, then it is easy to show that*:*

$$Y = \sqrt{\frac{P}{2}} T b_0 + \eta$$

Where $b_0 = \pm 1$ are the unknown possible values for the bit transmitted in [0,T) and η is a random Gaussian variable with zero mean value and variance equal to $\frac{N_0 T}{4}$

The detector is an non linear zero-threshold hard limiter providing as an output +1 if Y>0 and -1 if Y<0.

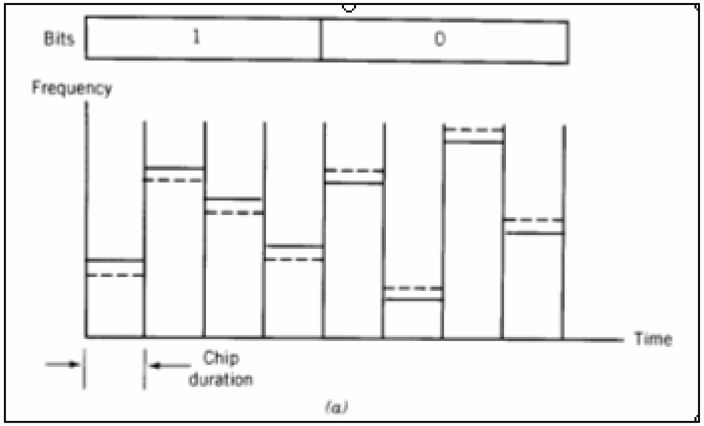
Frequency Hopping (FH)

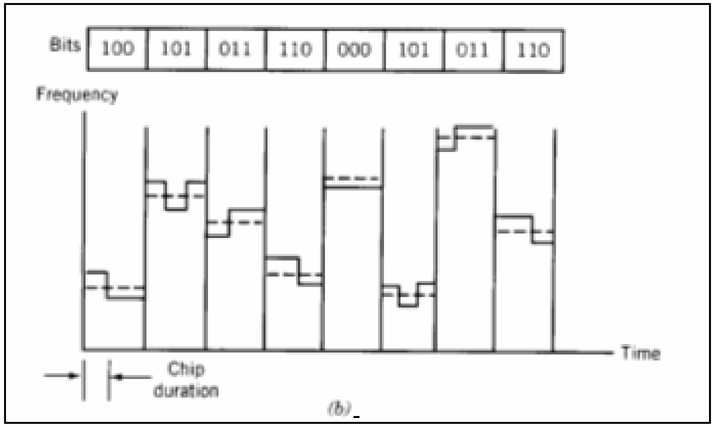
A FH transmitter periodically changes carrier frequency according to an a-priori code. The element time slot of the hopping sequence, during which the transmitted signal remains on the same carrier is called Hop Time (T_h).

For instance, if the narrow band signal has a bandwidth of 100 KHz and the SS bandwidth is 100 MHz, the transmitter could change carrier frequency among 1000 different values.

Depending on Hop Time T_h and Bit time Tb of the data signal, it is possible to identify two different types of FH:

- ***SLOW FH (SFH)*** (right) if more than one consecutive data bit is transmitted over the same carrier, i.e. $T_b < T_h$.
- ***FAST FH (FFH)*** (left) if one bit is sent over several hops in a PN sequence, i.e. $T_b > T_h$,





FH Transmitter

The transmitter first moves the signal to a reference carrier frequency and then moves it at frequency offsets described in the periodical PN code. It is composed by:

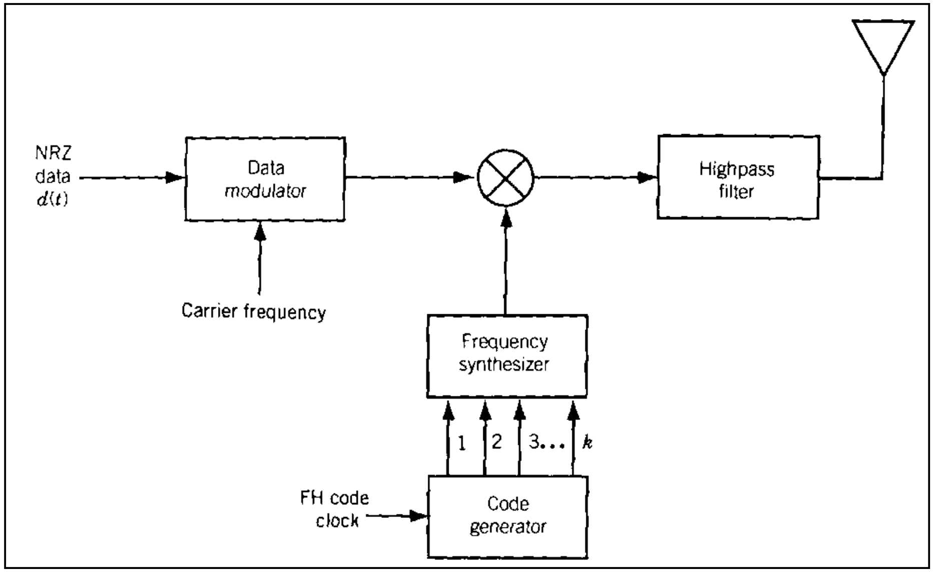
Data modulator : e.g. a BPSK modulator, that modulates the signal at an initial carrier frequency f_0.

Code Generator : generating a periodic pseudo-random sequence whose kth element represents the frequency hop Δf_k to be used at step k of the sequence.

Frequency Synthesizer : it uses the carrier corresponding to hop Δf_k to re-modulate the initial carrier frequency by multiplication in time domain (shift in frequency) .

The signal remains at frequency $f_0 + \Delta f_k$ during the corresponding Hop Time.

Highpass filter: it removes undesired spectral content generated by previous step outside the signal passband.



FH Receiver

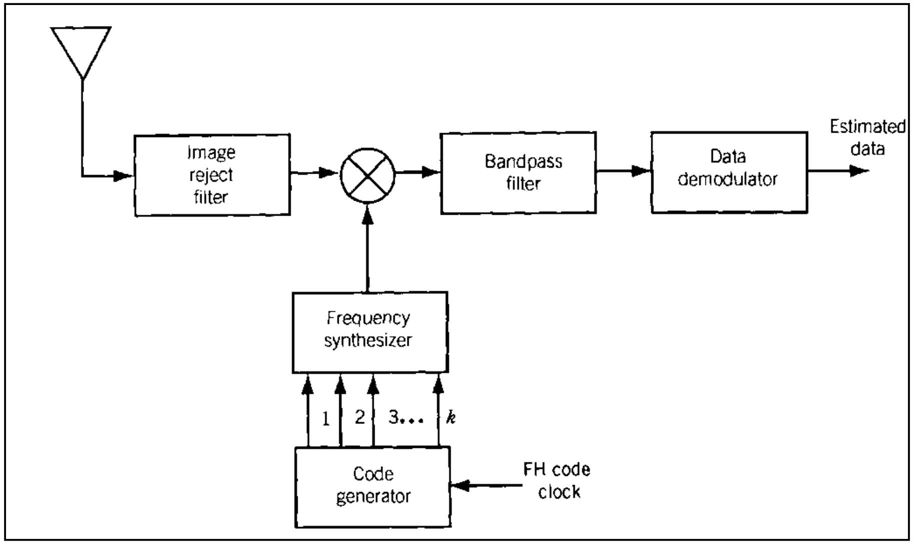
The receiver after removing content out of the bandwidth of interest, then first passband despread the signal by moving back all shifts at the carrier frequency and then performs narrowband demodulation. It is composed by:

Image Reject Filter to remove signals outside passband of interest.

Code Generator and the ***Frequency Synthesizer*** provide the same PN code used at the transmitter to obtain Frequency Hops necessary for despreading around frequency f_0.

Band Pass Filter allows to reject undesired signal replicas generated by frequency shift in adjacent bands.

Demodulator: e.g. BPSK de-modulates the signal to allow data baseband estimation



DS-SS vs FH-SS

• Bandwidth occupancy for DS-SS is $2 f_{chip}$, where f_{chip} is chip frequency. To obtain higher bandwidth (i.e. higher *P*, thus reducing interference) higher chip frequencies are necessary; consequently, time synchronization become more complex as well as energy consumption due to higher computational load.

• In FH-SS, bandwidth occupancy is related to the range within which frequency hops can vary. Compared to DS-SS, it is simpler to obtain larger bandwidth and process gain. Frequency synchronization can be necessary in time variant channels.

• Synchronization procedures are more difficult in DS than FH. In FH hops can change few thousands time per second, whereas for DS the chip frequency reaches several MHz.

•DS-SS signal frequency content is time invariantly fully spread on a wide-band spectrum, whereas in FH-SS spreading consists of periodically shifting a narrow-band modulated signal onto a wide range of carriers.

DS-SS Performances in Noisy Environments (1/5)

White Gaussian Noise

Let's first consider the performances on a DS-SS receiver, in case the only noise affecting the signal is a zero mean additive White Gaussian Noise, *n(t).* In this case one can write r(t)=s(t)+n(t) as the signal that is provided at the DS-SS receiver. The variable Y at the output of the matched filter can be written as $Y = s_0 + n_0$, to indicate the signal and the noise components.

If $A = \sqrt{P}$ is data amplitude of a bit at data rate 1/T, then: $s_0 = \pm \frac{AT}{2}$

The noise after matched filter is: $n_0 = \int_0^T n(t)\, p(t) \cos(2\pi f_c t) dt$

Auto-correlation of AWGN is: $R_n(\tau) = E\{n(t)n(t+\tau)\} = \frac{N_0}{2}\delta(\tau)$

After filtering noise variance is : $\mathrm{var}(n_0) = E(n_0^2) = E\left\{\left[\int_0^T n(t)\, p(t) \cos(2\pi f_c t) dt\right]^2\right\} = \frac{N_0 T}{4}$

It is worth mentioning that the process gain **P has no influence on the previous values**.

DS-SS Performances in Noisy Environment (2/5)

Now it is possible to define the **Signal to Noise Radio** (SNR):

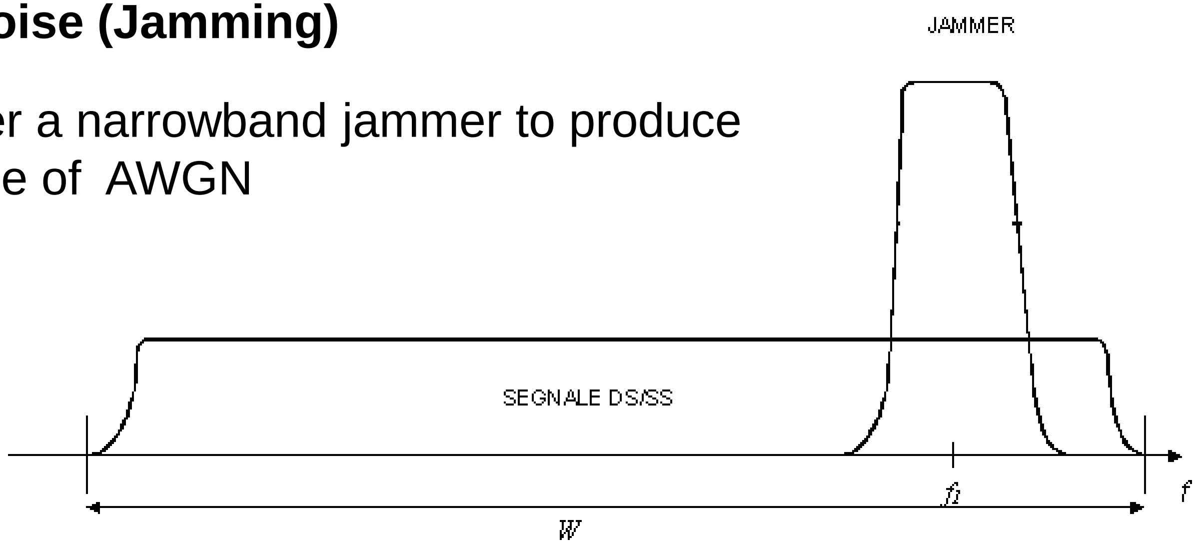
$$SNR_{out} = \frac{s_0^2}{E(n_0^2)} = \frac{A^2T^2}{4}\frac{4}{N_0T} = \frac{A^2T}{N_0} = 2\frac{E_b}{N_0}$$

The results show that SNR obtained with **DS-SS with BPSK and AWGN** has the same value as the simple narrowband BPSK system.

DS-SS Performances in Noisy Environments (3/5)

Narrow Band Noise (Jamming)

Let us now consider a narrowband jammer to produce interference in place of AWGN



A jamming signal can be defined as: $J(t) = S_J(t)\cos(2\pi f_1 t + \psi)$,

where $S_j(t)$ is stationary, zero mean, pass-band random process and ψ is a random variable uniformly distributed between (0,2π).

In this case one can write $Y = s_0 + j_0$.

The noisy component due to the jammer output from the matched filter is:

$$j_0 = \int_0^T S_J(t)\,p(t)\cos(2\pi f_1 t + \psi)\cos(2\pi f_c t)\,dt$$

DS-SS Performances in Noisy Environments (4/5)

The jamming autocorrelation function is:

$$R_J(\tau) = E\{J(t)J(t+\tau)\} = \frac{1}{2} R_{SJ}(\tau)\cos(2\pi f_1 t)$$

Where $R_{SJ}(\tau)$ is the auto correlation of $S_J(t)$.

The mean power of the jammer can be written as $\overline{P}_{S_J} = R_{S_J}(0)$.

The variance of j_0, useful to model noise power, can be computed by noting that the jammer power is spread at the receiver after multiplication with PN code. So, the higher the process gain the higher the dispersion of jammer power on signal bandwidth

It can be shown that SNR in this case can be written as:

$$SNR_{out} = \frac{s_0^2}{E(j_0^2)} = \frac{A^2 T^2}{4} \frac{4P}{\overline{\overline{P_{SJ}}} T^2} = \frac{A^2}{\overline{\overline{P_{SJ}}}} P = P\left(\frac{S}{I}\right)_{narrowband}$$

In case of narroband noise (that can also represent frequency fading) the higher the Process Gain ***P*** **the higher SNR with respect to SNR for an equivalent narrowband modulation** affected by the jammer

DS-SS Performances in Noisy Environments (5/5)

Broad Band Noise

Let us now consider as noise the interference of another wide band signal (either another DS user or a self interfering replica of the same user) to be present at the receiver. Let us that the amplitude/power of the user and of the interfering signal are the same.

The received signal can now be written as: $r(t) = s(t) + J(t) = Ac(t)\,p(t)\cos(2\pi f_c t) + Ac'(t-\tau')\,p'(t-\tau')\cos(2\pi f_c t + \theta')$

The output of the matched filter is again $Y = s_0 + j_0$. However now, we have:

$$j_0 = A\int_0^T c'(t-\tau')\,p'(t-\tau')\,p(t)\cos(2\pi f_c t + \theta')\cos(2\pi f_c t)\,dt = \frac{A}{2}\cos(\theta')\int_0^T c'(t-\tau')\,p'(t-\tau')\,p(t)\,dt =$$

$$\frac{AT}{2}\cos(\theta')\left[\pm\frac{1}{T}\int_0^{\tau'} p'(t-\tau')\,p(t)\,dt \pm \frac{1}{T}\int_{\tau'}^{T} p'(t-\tau')\,p(t)\,dt\right]$$

Jo is here defined as ***Single-User Interference.***

The simultaneous presence of several instances of jo (e.g. coming from different users) can be defined as ***Multiple Access Interference – MAI.***

It can be shown that in this case : $\mathrm{var}(j_0) = \dfrac{A^2T^2}{4} F\left(P, R_{p'p}(\tau)\right)$

DS-SS in Multipath Environments

A specific example of broad band noise in DS-SS is self interference among multipath replicas. For example, in such cases the received signal is the sum of the spread direct component (LOS) and of the noise components, i.e. the also spread delayed signal replicas.

Due to PN-sequence autocorrelation the noise generated by the replica can be rejected if the replica delay τ wrt LOS is larger than the chip time T_C,

i.e. $\tau > T_C$. In fact the chip time is also the memory of PN codes.

So, if the minimum delay of the signal replicas can be estimated and it is possible to fix a chip time lower than it, then the self-interference of the replicas on the LOS component could be completely removed. The same could be done for all possible replica pairs delayed by at least Tc. For example, in indoor channels delay can be estimated to vary between 200-500 nsec. Unfortunately, in many real-life environments it is not possible to estimate minimum delay.

The ***Rake Receiver takes advantage from this by spacing replicas of at least Tc=1/W.***

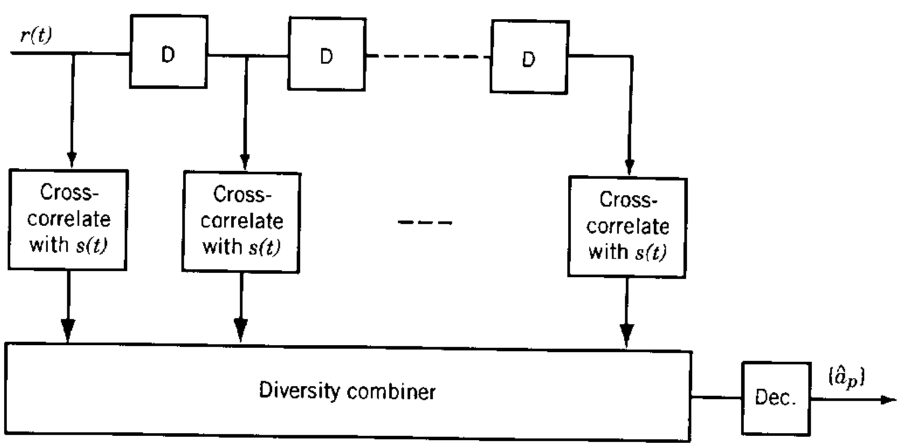
Rake Receiver

In a Rake Receiver, the energy from each informative signal replica is separately considered and processed. In particular, received signal goes first through a tapped delay line, where each tap delays the input by *D* seconds. Usually $D=T_c$ or $D=T_c/2$ *or* the delay *D* can be dynamically computed.

The relative delay $|\tau_k - \tau_l|$ between two replicas k and l as compared to the spread signal bandwidth determines if the two replicas can be considered self-interfering.

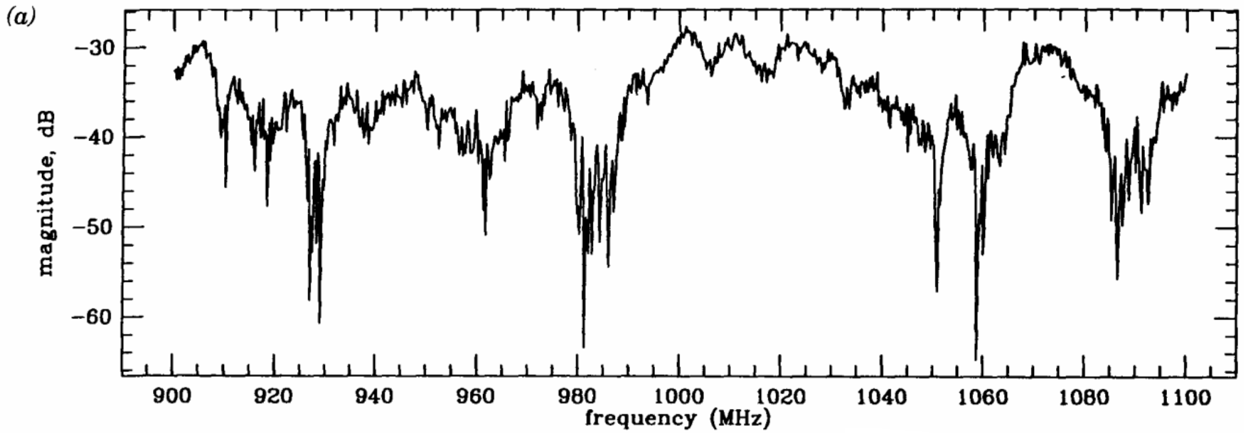
If $|\tau_k - \tau_l| > \frac{1}{W} = T_c$ than the two replicas codes will generate a null outcome from the matched filter

The larger the bandwidth, the higher the number of replicas that can be 'solved' in a self interference robust way by the rake receiver. However, often Tc cannot be reduced below a given threshold due to time synchronization issues.



FH-SS in Multipath Environments (1/2)

Also by using FH-SS good robustness to self-interference can be obtained. It has to be recalled that multipath wireless channel nature produce frequency selectivity. So at a given time a possible frequency response is like the one plot in the following figure.



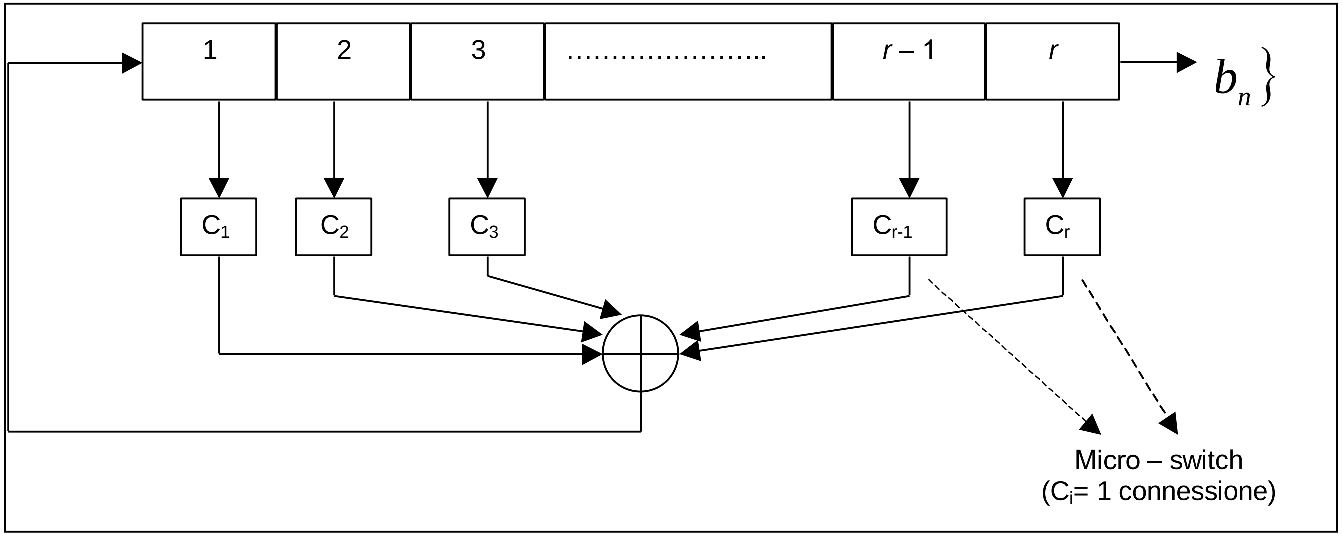
The dropped frequencies correspond to frequencies randomly selected by the channel to be faded at a given time As FH hops onto different frequencies in time the probability of being affected by severe fading on a single bit transmission can be reduced by reducing the hop time (Fast hopping).

FH-SS in Multipath Environments (2/2)

- **In case of Slow FH**, one or more bits can be completely corrupted by multipath in case of collision of hop frequency and fading. High Bit Error Rate (BER) can be generated that can arrive to interrupt link. By using source coding like convolutional FEC or interleaving, this problem can be reduced.
- **In case of Fast FH**, only parts of bits are affected by fading as the information content is spread on to multiple hop frequencies. If successive hops are spaced more than coherence bandwidth the probability that fading affects strongly consecutive hops can be reduced. Therefore better performances can be obtained than Slow-FH, despite at the price has to be paid of more energy for higher hop frequency.

PN Sequences (1/3)

PN generators are needed in transmitters and receivers for both DS and FH. The pseudo noise sequences can be generated starting from r-stages shift registers as in figure. Each shift register is composed by r elements containing sequence symbols (generally binary values). When the register content is shifts right a new element of a PN sequence is produced.



The output of the register is a sequence *bn*: $b_n = C_1 b_{n-1} \oplus C_2 b_{n-2} \oplus \ldots\ldots \oplus C_r b_{n-r}$

The coefficients *Cr* can be 0 /1 depending on the specific code.

NB: r is the length of the shift register and NOT of the sequence.

PN Sequences (2/3)

The PN sequence is a pseudo *random sequence*. It can be proven that the sequence so generated is such that :

$$\Pr(b_n = 1) = \frac{1}{2}(1 - s) \qquad \Pr(b_n = -1) = \frac{1}{2}(1 + s)$$

where $s \triangleq \frac{1}{2^{r-1}}$ is the statistical displacement.

If the number of elements r becomes larger than s is reduced and the sequence is fully unpredictable at each element.

Generally the sequence is represented by binary values (0,1).

However the waveform of the PN code can be easily obtained by mapping (0,1) into a bipolar (-1,+1) sequence and by including a PAM codec setting pulse duration equal to Tc.

PN Sequences (3/3)

It can be shown that under particular conditions the obtained sequences are periodic. The period L is the length of PN sequence

If a PN generator is used to produce PN codes, the period L becomes the process Gain N as it can be interpreted as the number of chips inside a bit.

A particular maximum value of the period can be obtained when the characteristic polynomial

$$P(x) = 1 + C_1 x + C_2 x^2 + ... + C_r x^r$$

is prime and when the shift register is initialized by assigning the following binary values to its r elements:

$$(b_{10}, ..., b_{r0}) = (0,0,......,01)$$

In such a case it can be shown that the period of the PN sequence is such that $L = N = 2^r - 1$

The sequence is called ***maximal length sequence*** (*m – sequence*).